

Application No. 09/609,197
Amendment "A" dated October 20, 2003
Reply to Office Action of July 30, 2003

AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph that begin at line 21 of page 13 with the following amended paragraph:

a1
Program code means comprising one or more program modules may be stored on the magnetic hard disk 139, removable magnetic disk 129, optical disk 131, ROM 124 or RAM 125, including an operating system 135, one or more application programs 136, other program modules 137, and program data 138. A user may enter commands and information into the computer 120 through keyboard 140, pointing device 142, or other input devices (not shown), such as a microphone, joy stick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 121 through a serial port interface 146 coupled to system bus 123. Alternatively, the input devices may be connected by other interfaces, such as a parallel port, a game port or a universal serial bus (USB). A monitor 147 or another display device is also connected to system bus 123 via an interface, such as video adapter 148. In addition to the monitor, personal computers typically include other peripheral output devices (not shown), such as speakers and printers.

Please replace the paragraph that begins on line 9 of page 16 with the following amended paragraph:

a2
The memory device such as memory device 208 that stores the object may be any memory device that the servers 206 have access to. By way of example, the memory device 208 may include any of the memory device described above for Figure 1 including ROM 124, RAM 125, removable magnetic disk 129, removable optical disk 131, ~~hard-magnetic~~ hard disk 139 or any other memory device. In some cases, the memory device 208 may represent multiple memory devices as when the object 210 is replicated or cached on several memory devices in order to allow the server network more efficient access to the object. The object 210 may essentially be any data structure including document files, executable files and so forth.

Application No. 09/609,197
Amendment "A" dated October 20, 2003
Reply to Office Action of July 30, 2003

Please replace the paragraph that begins on line 18 of page 20 with the following amended paragraph:

a3
Now that the security descriptors are consistent, any changes to one of the security descriptors are replicated to the other security descriptor. Figure 7 illustrates a method 700 for replicating changes in security descriptor #1 to security descriptor #2. The data structures involved with this replication are shown as they existed at instances of time sequentially beginning at Figure 8A and ending at Figure 8C. The method of Figure 7 will now be described with reference to the data structures of Figures 8A, 8B and 8C.

Please replace the paragraph that begins on line 18 of page 22 with the following amended paragraph:

a4
The method of Figure 7 is then implemented except that changes to the security descriptor #2 are now made to replicated to the security descriptor #1. Specifically, ~~in step 710,~~ the security descriptor #2 that follows the specification #2 is converted into a version of the security descriptor #2 that follows the specification #1 as shown in Figure 9B. Using the mapping rules, right A' maps to right A, the combination of rights C.1' and C.2' map to right C, right D' maps to right D, and right E' maps to the combination of rights E.1 and E.2 to form the version of the security descriptor #2 that follows the specification #1. Next, this version is compared to the security descriptor #1 that also follows the specification #1 to reveal that right C is added and right !D is changed to right D. These changes are then implemented in the security descriptor #1 as shown in Figure 9C.

Please replace the paragraph that begins on line 4 of page 18 with the following amended paragraph:

a5
The server network 202 is thus a security heterogenic computer network. In this description and in the claims, a network in which different security descriptor specifications are used when determining security permissions is referred to as a "security heterogenic computer network." A security heterogenic computer network may occur when different software is

Application No. 09/609,197
Amendment "A" dated October 20, 2003
Reply to Office Action of July 30, 2003

AS
running on the servers within the network. For example, some of the server such as server 206a may be running MICROSOFT ® WINDOWS NT ® workstation 4.0 or server 4.0 operating systems or perhaps MICROSOFT ® Exchange version 5.5 communication software. Each of these software packages uses the 4.0 security descriptor specification. On the other hand, other servers such as server 206b may be running MICROSOFT ® WINDOWS ® 2000 operating system or MICROSOFT ® Exchange 2000 communication software which use the Active Directory security descriptor specification.
